(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10255121 A**

(43) Date of publication of application: **25 . 09 . 98**

(51) Int. Cl **G07F 7/12**
G06F 17/60
G06K 17/00

(21) Application number: **09055239**

(22) Date of filing: **10 . 03 . 97**

(71) Applicant: **GLORY LTD**

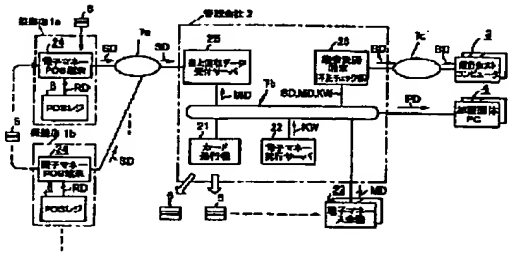
(72) Inventor: **KAMISE YOUJIROU**

(54) **ELECTRONIC MONEY SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To detect dishonesty such as the forgery/alteration of a card in a money payment process or the alteration of sales data in a store, and to ensure security by checking dishonesty from sales data and the data of an electronic money issuing device or the like, totaling a payment sum to the store, and transmitting it to the computer of a bank for a payment processing.

SOLUTION: An electronic money issuing server 22 stores/manages data such as security information KW such as the password of a card owner. A sales collection data accepting server 25 receives and stores money data MD paid to a pre-paid card 5 by an electronic money paying machine 23 and sales data SD stored in an electronic money POS terminal. A total settling terminal 26 checks the alternation of data based on the security information KW, sales data SD, and money data MD, totals a payment sum to the store, and transmits transfer data BD to a bank host computer 3 for a payment processing.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－255121

(43)公開日　平成10年(1998)９月25日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｃ
Ｇ０６Ｆ　17/60		Ｇ０６Ｋ　17/00	Ｌ
Ｇ０６Ｋ　17/00		Ｇ０６Ｆ　15/21	３４０Ａ

審査請求　未請求　請求項の数３　ＯＬ　（全 12 頁）

(21)出願番号　特願平9－55239

(22)出願日　平成９年(1997)３月10日

(71)出願人　000001432
グローリー工業株式会社
兵庫県姫路市下手野１丁目３番１号

(72)発明者　神瀬　陽二郎
兵庫県姫路市下手野一丁目３番１号　グローリー工業株式会社内

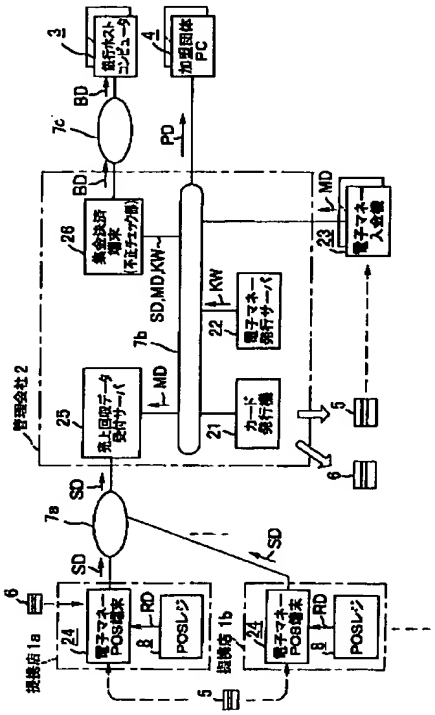
(74)代理人　弁理士　安形　雄三

(54)【発明の名称】　電子マネーシステム

(57)【要約】

【課題】　金銭的価値を記憶させたカードによる金銭支払いの課程に於ける様々な不正を検出し、セキュリティを確保することができる電子マネーシステムを提供する。

【解決手段】　ＩＣカード５に金銭的価値を記憶させると共に、発行の番号を付して発行する電子マネー発行装置２１，２３と、商品の購入の際に前記ＩＣカードによる支払い処理を行うための電子マネーＰＯＳ端末２４と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段２２と、前記電子マネーＰＯＳ端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段２５と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該当店舗の支払い金額を集計して銀行のコンピュータ３に送信し実支払い処理を行う集計決済コンピュータ２６とを備える。



1

【特許請求の範囲】

【請求項１】　現金若しくは後払い契約によりＩＣカードに金銭的価値を記憶させると共に、購入者が使用する際の暗証番号を受付けると共に発行の番号を付して前記ＩＣカードに記憶させて発行する電子マネー発行装置と、商品の販売店若しくはサービスの提供場所に設けられ、商品の購入の際に前記ＩＣカードによる支払い処理を行うための電子マネーＰＯＳ端末と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段と、前記電子マネーＰＯＳ端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該当店舗の支払い金額を集計して銀行のコンピュータに送信し支払い処理を行う集計決済コンピュータとを備えたことを特徴とする電子マネーシステム。

【請求項２】　利用者ＩＣカードを受付けて内部に記憶されているパスワードを読出すと共にプリペイド金額を読出し更新するＩＣカードリードライタと、少なくとも販売金額を入力するための売上金額入力手段と、利用者が暗証番号を入力するための暗証番号入力手段と、ガイダンス及び入力した金額を表示するための表示手段と、所定期間の売上データを記憶する記憶手段と、前記利用者ＩＣカードを読出した際には、該カード内部に記憶されている暗証番号と前記暗証番号入力手段より入力された利用者の暗証番号とが一致した場合に前記プリペイド金額を更新すると共に、該カード内部に記憶されている暗号キーによって利用者の支払いデータを暗号化して、同一情報で暗号化しないものを回収データとして前記暗号化されたデータとともに前記記憶手段に記憶し、店所有のＩＣカードを読出した際には、前記記憶手段に記憶されている回収データを該店所有のＩＣカードの暗号化プログラムによって暗号化し、２種類の暗号化データを前記売上データとして所定期間分前記記憶手段に記憶させ、ホストコンピュータに電話を掛けて前記売上データを転送する制御部とを有する電子マネーＰＯＳ端末を具備したことを特徴とする電子マネーシステム。

【請求項３】　利用者により入力されたＩＣマネーカードの暗証番号によりカード所持者の個人認証を行う第１の認証手段と、前記ＩＣマネーカードに記録された暗号化プログラム及び第１の暗号キーにより利用金額を暗号化する第１の暗号化手段と、店舗担当者により入力された店舗用カードの暗証番号により取扱担当者の認証を行う第２の認証手段と、前記店舗用カードに記録された暗号化プログラム及び第２の暗号キーにより前記利用金額に対する売上金額を暗号化する第２の暗号化手段と、前記第１及び第２の暗号化手段によりそれぞれ暗号化された前記利用金額と売上金額の一対の暗号化データを纏めて送信する送信手段とを有する電子マネーＰＯＳ端末

2

と；前記電子マネーＰＯＳ端末からの前記一対の暗号化データを予め登録された第１及び第２の解除キーを用いてそれぞれ復号して両データの一致を確認すると共に、前記ＩＣマネーカードの金銭的価値データを書換える電子マネー入金機からの入金金額データ及び前記復号された利用金額データに基づき、前記ＩＣマネーカードに対する入金と出金との大小関係を比較して入出金の正当性を確認する不正検出手段を有する管理コンピュータと；を備えたことを特徴とする電子マネーシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣカードをプリペイドカードとして使用した電子マネーシステムに関し、特に、金銭的価値を記憶させたカードによる金銭支払いの課程に於ける各種のデータ改ざんを検出し、セキュリティを確保し得るようにした電子マネーシステムに関する。

【０００２】

【従来の技術】現在、カードを用いて商品の購入や各種サービスの利用をできるようにしたキャッシュレス・システムとしては、プリペイドカード・システム，クレジットカード・システム，銀行ＰＯＳシステムといった様々なシステムが普及しており、近年では、いわゆる電子マネーによる取引を可能とした電子マネーシステムが実現されつつある。これらのキャッシュレス・システムでは、利用者が商品を購入してから決済が完了するまでの過程において様々な不正行為がなされる可能性がある。そこで、金銭的価値データを記録する媒体として磁気カードなどの媒体に比べて安全性の高いＩＣカードを用いるようにしたシステムが数多く開発されている。

【０００３】ＩＣカードを用いたプリペイドカード・システムとしては、例えば特開平４－３１３１９０号公報に開示されている。このシステムは、銀行（銀行センターシステム）、利用者（ＩＣカード）、及び店舗（取引端末）とでプリペイドカードシステムを構成しており、ＩＣカードによる買物が行われるごとに、買物金額を加算して売上合算を計算し、そのデータを取引端末若しくはＩＣカードに格納してある銀行鍵を使用して暗号化し、売上合算データとその暗号文を取引端末に格納する。そして、次回からは売上合算を算出する際に前回の売上合算データを暗号化して暗号文と比較、或いは暗号文を復号して売上合算データと比較し、データの改ざんがないか否かを判定する。そして、銀行センターシステムでは、取引端末から一定期間毎に送られてくる決済要求に対して取引端末と同一のロジックで売上合算データと暗号文とを照合し、一致していれば不正改ざんがないと判断して決済処理を実施するようになっている。しかしながら、この場合は店側でデータを暗号しているので、店側で売上データを改ざんすることが可能である。

【０００４】一方、銀行とは異なる機関において、ＩＣ

カードをプリペイドカードとして際の代金の精算業務を行うようにしたシステムとしては、例えば特開平５－３２４９９８号公報に記載のものが挙げられる。このシステムは、加盟店共通の事務局（ホストコンピュータ）を設け、顧客に配布したＩＣカードとのやりとりを行うことができるリーダ／ライタ装置を各加盟店に配置し、リーダ／ライタ装置とホストコンピュータとの間で情報の伝達を行い、代金の精算を集中管理するようにしたものである。このシステムにおいては、各顧客は事務局において住所や氏名を登録し、所定のプリペイド額を支払ってＩＣカードを受取り、代金精算は加盟店からの取引情報がホストコンピュータに送られてきた取引情報に基づき行われる。また、顧客のＩＣカードにはプリペイド残額の他に、売掛金残額やサービスポイント残額が記録されるようになっており、売掛金計上による支払いやサービスポイントからの支払いを可能としている。しかしながら、当公報には、セキュリティに関する技術内容に関した記載は何もない。

【０００５】また、ＩＣカードをプリペイドカードとして用い、プリペイドカードの残金を更新することで再利用できるようにしたシステムとしては、例えば特開平３－２６６０９５号公報に記載のものが挙げられる。この実施例に記載のキャッシュレスシステムは、銀行のホストコンピュータに接続されるプリペイド記録機と、銀行のホストコンピュータに接続される管理会社のコンピュータと、各店舗内に配置される専用端末とから構成される。そして、暗証番号を入れることにより読み書きが可能となるＩＣカードを使用して、銀行のホストコンピュータに接続して暗証番号を入力してＯＫであれば自分の銀行口座から管理会社への振替金額であるプリペイド金額をＩＣカードに書き込む。店でカードを使う際には、カードを専用端末に装着して暗証番号を入れた後に利用金額分を減算してカードのプリペイド金額を減算する。また、専用端末はカードが装填されたときには、管理会社のコンピュータと接続されていて所定期間毎に利用金額と店舗を示す情報を出力する様にしている。

【０００６】

【発明が解決しようとする課題】上述した従来のシステムでは、一般的な暗証番号による個人認証や銀行鍵を用いてデータ照合を行っていることが一部の公報に開示されている。しかしながら、データの改ざんに対する保証については詳しい記載がなく、店側とかデータの伝送時の安全保護については何も対策が講じられていない。企業内等の使用場所が限られたエリア内で適用する場合には、従来のシステムにおいても比較的セキュリティが確保されると言えるが、一般の店舗などにも利用範囲を拡張して適用する場合には、暗号等が解読されて一部のセキュリティが破れても、その不正を検出して取引を中止させることができるような、より安全性をきわめたシステムを構築して提供することが重要な課題と言える。

【０００７】本発明は上述のような事情から成されたものであり、本発明の目的は、金銭的価値を記憶させたマネーカードによる金銭支払いの課程に於ける、カードの偽造／変造，店舗内における売上データの改ざん，伝送時のデータの改ざんなどの不正を検出し、セキュリティを確保することができる電子マネーシステムを提供することにある。

【０００８】

【課題を解決するための手段】本発明は、ＩＣカードをプリペイドカードとして使用した電子マネーシステムに関するものであり、本発明の上記目的は、現金若しくは後払い契約によりＩＣカードに金銭的価値を記憶させると共に、購入者が使用する際の暗証番号を受付けると共に発行の番号を付して前記ＩＣカードに記憶させて発行する電子マネー発行装置と、商品の販売店若しくはサービスの提供場所に設けられ、商品の購入の際に前記ＩＣカードによる支払い処理を行うための電子マネーＰＯＳ端末と、前記電子マネー発行装置のデータを記憶し管理するカード発行サーバ手段と、前記電子マネーＰＯＳ端末から回線を通じて情報の供与を受ける売上回収データ受付サーバ手段と、前記回収データ受付サーバ手段の記憶している売上データと前記カード発行サーバ手段のデータと前記電子マネー発行装置のデータとから不正のチェックをした後、該当店舗の支払い金額を集計して銀行のコンピュータに送信し支払い処理を行う集計決済コンピュータとを備えることによって達成される。

【０００９】或いは、利用者ＩＣカードを受付けて内部に記憶されているパスワードを読出すと共にプリペイド金額を読出し更新するＩＣカードリードライタと、少なくとも販売金額を入力するための売上金額入力手段と、利用者が暗証番号を入力するための暗証番号入力手段と、ガイダンス及び入力した金額を表示するための表示手段と、所定期間の売上データを記憶する記憶手段と、前記利用者ＩＣカードを読出した際には、該カード内部に記憶されている暗証番号と前記暗証番号入力手段より入力された利用者の暗証番号とが一致した場合に前記プリペイド金額を更新すると共に、該カード内部に記憶されている暗号キーによって利用者の支払いデータを暗号化して、同一情報で暗号化しないものを回収データとして前記暗号化されたデータとともに前記記憶手段に記憶し、店所有のＩＣカードを読出した際には、前記記憶手段に記憶されている回収データを該店所有のＩＣカードの暗号化プログラムによって暗号化し、２種類の暗号化データを前記売上データとして所定期間分前記記憶手段に記憶させ、ホストコンピュータに電話を掛けて前記売上データを転送する制御部とを有する電子マネーＰＯＳ端末を具備することによって達成される。

【００１０】或いは、利用者により入力されたＩＣマネーカードの暗証番号によりカード所持者の個人認証を行う第１の認証手段と、前記ＩＣマネーカードに記録され

た暗号化プログラム及び第１の暗号キーにより利用金額を暗号化する第１の暗号化手段と、店舗担当者により入力された店舗用カードの暗証番号により取扱担当者の認証を行う第２の認証手段と、前記店舗用カードに記録された暗号化プログラム及び第２の暗号キーにより前記利用金額に対する売上金額を暗号化する第２の暗号化手段と、前記第１及び第２の暗号化手段によりそれぞれ暗号化された前記利用金額と売上金額の一対の暗号化データを纏めて送信する送信手段とを有する電子マネーＰＯＳ端末と；前記電子マネーＰＯＳ端末からの前記一対の暗号化データを予め登録された第１及び第２の解除キーを用いてそれぞれ復号して両データの一致を確認すると共に、前記ＩＣマネーカードの金銭的価値データを書換える電子マネー入金機からの入金金額データ及び前記復号された利用金額データに基づき、前記ＩＣマネーカードに対する入金と出金との大小関係を比較して入出金の正当性を確認する不正検出手段を有する管理コンピュータと；を備えることによって達成される。

【００１１】

【発明の実施の形態】本発明は、従来、企業内等の使用場所が限られたエリア内でセキュリティが確保されて使用していたプリペイドカードを近郊の提携店でも使用できるようにしたものである。提携店側の売上データをセンター側で収集して決済処理などを行うシステムを構築する場合には、提携店側での売上データの改ざんや通信上でのデータ盗取による通信データの改ざんなど、プリペイドカードが使用可能な全てのエリアにおける不正行為を防止し、システムのセキュリティを確保する必要が生じる。本発明では、ＩＣカードを電子マネーを格納する媒体として使用し、先ず、利用客のＩＣカードに記憶されている第１の暗号キーを基に利用客の支払いデータを暗号化することによって、店側での支払いデータの改ざんを防止する。次に、店側では、客の支払い金額と同額の回収金額のデータに対して店長等の店舗専用のＩＣカードに記憶されている第２の暗号キーを基に暗号化した回収データを作成する。これらの暗号化は、例えばカード所持者により入力される暗証番号を上記の暗号キーとして、ＩＣカードに予め記録されている暗号化プログラムによって行なわれる。そして、暗号化された回収データと支払いデータを１対にして、売上データとして公衆電話回線等の通信回線を通じて管理会社のサーバ（売上回収データ受付サーバ）に電送する。

【００１２】ここで、管理会社とは店側への支払いを代行するとともに、金額の追加及び払い戻しが可能なプリペイドカードを利用者に販売し、店独自の特典や広告などの各種サービスを提供する機関であり、銀行とは異なる機関である。管理会社では、電送元の店の番号を基に、別サーバ（電子マネー発行サーバ）に登録されている復号キーを検索し、この復号キーを基に暗号を解いて復号された回収データを得、次いで回収データに含まれる利用者のＩＤコードより、上記の別サーバに登録されている利用者毎の暗号キーを検索してこれを基に支払いデータを復号し、復号された回収データと支払いデータとを請求データとして記憶する。この時点で支払いデータと回収データとが一致することを確認する。これにより、管理会社に電送される際の傍受によってデータが改ざんされて悪用されることを防止している。

【００１３】更に、電子マネーＩＤを付与して利用者カードの入出金のログを記録し、このログデータに基づいてプリペイドカードの販売金額（ＩＣカードに入金された金額）とそのプリペイドカードによって支払われた金額（利用者の利用金額）の大小関係をチェックすることによって、プリペイドカードの改ざんがなされたことがあるかどうか等の総合的なチェックを行う。更に又、提携店へ確認の帳票を送付し、管理会社の集計決済端末は、提携店側での確認がＯＫであれば、利用者の利用金額（即ち店の請求金額）を店の銀行口座へ振り込む様にしている。このように、本発明では各種の不正のチェックを行うことにより詐欺による電子マネー（ＩＣプリペイドカード）システムの不正使用を防ぐようにしている。

【００１４】以下、図面に基づいて本発明の好適な実施の形態について詳細に説明する。図１は本発明の電子マネーシステムの全体構成の一例を示している。図１において、管理会社（プロバイダー）２は、コンビニエンスストア，書店，飲食店等の提携店１（１ａ，１ｂ，…）での利用が可能で且つ金額の追加が可能なプリペイドカード（電子マネーカード）５を発行し、提携店１からの売上データを集計して各種不正のチェックを行い、該当店舗への支払い金額を店の銀行口座へ振り込む等のサービスを提供する機関である。本システムの利用者は、管理会社２に加盟している団体（学校や勤め先等：以下「加盟団体」と言う）の一員（学生，従業員等）である。プリペイドカード５は、専用のカードとしても良く、社員カードや会員制カードをプリペイドカード５として使用できるようにしても良い。本例では、暗号化プログラムを記録したＩＣカードを用いており、暗号化のアルゴリズムとしては、ＤＥＳ（ｄａｔａ　ｅｎｃｒｙｐｔｉｏｎ　ｓｔａｎｄａｒｄ）型アルゴリズムを用いている。

【００１５】管理会社２が提供する電子マネーシステムは、利用者が所持するプリペイドカード（ＩＣマネーカード：以下、「ＩＣカード」とする）５及び店舗用ＩＣカード６を発行するカード発行機２１と、セキュリティ情報（カード所持者のパスワードやＩＣカード５，６の暗号解読キー等）ＫＷ等のデータを記憶／管理する電子マネー発行サーバ２２と、ＩＣカード５への入金（電子マネーのチャージ）を行うための電子マネー入金機２３と、ＩＣカード５による支払い機能を有する電子マネーＰＯＳ端末２４と、電子マネー入金機２３によりＩＣカ

ード５へ入金された入金データＭＤ及び電子マネーＰＯＳ端末２４に蓄積された売上データＳＤを受信して記憶する売上回収データ受付サーバ２５と、セキュリティ情報ＫＷ，売上データＳＤ及び入金データＭＤに基づいてデータの改ざん等の不正（カード偽造，ＰＯＳ端末に記憶されているデータの改ざん，伝送データの改ざん等）のチェックをした後、該当店舗への支払い金額を集計して銀行のコンピュータ３に振込データＢＤを送信し、支払いの処理を行う集計決済端末２６とを備えている。

【００１６】各提携店１（１ａ，１ｂ，…）側に設置される電子マネーＰＯＳ端末２４は、公衆電話回線７ａを介して管理会社２側に設置される売上回収データ受付サーバ２５と接続され、所定の場所に設置される電子マネー入金機２３とその他の装置（カード発行機２１，電子マネー発行サーバ２２，売上回収データ受付サーバ２５及び集計決済端末２６）は専用線７ｂを介して相互に接続されている。また、必要に応じて専用線７ｂを介して、給与天引きのデータＰＤを処理する加盟団体のコンピュータ（パーソナルコンピュータ又は企業等のセンタコンピュータ等）４が専用線７ｂを介して接続される。この加盟団体のコンピュータ４には、フレキシブルディスク等の記憶媒体を用いてデータを送ることもできる。更に、集計決済端末２６は、専用線若しくは公衆回線を用いたネットワーク７ｃを介して銀行ホストコンピュータ３に接続されている。なお、各提携店１内の既存のＰＯＳレジの売上データＲＤは、手入力で電子マネーＰＯＳ端末２４に入力される。以下、本発明に係る電子マネーシステムの主要部の構成例についてそれぞれ説明する。

【００１７】図２は電子マネー入金機２３の構成の一例を示しており、図３はその外観図を示している。図２において、電子マネー入金機２３は、電子マネーに替える紙幣の受入れ及び釣り銭の返却処理をする紙幣入金ユニット２３２と、ＩＣカードのデータの読込み及び電子マネーデータ等の書換えを行うためのＩＣカードリーダライタ２３３と、ガイダンス表示や入金等の操作を行うためのタッチパネルを装着した表示装置２３４と、電子マネー残高等の明細をジャーナル印字するためのプリンタ２３５と、店舗案内表示サービス中には選択した店へ無料で電話をして予約等を行うことができ、また操作中に故障が起きた場合などに担当者と連絡をとるための電話機２３６と、管理会社２側の売上回収データ受付サーバ２５とオンライン接続するための通信装置２３７と、各機器を制御するパソコンから成る制御部２３１とを備えている。また、電子マネー入金機２３は無停電電源装置４０を具備しており、各機器は無停電電源装置４０を介して電源に接続されている。

【００１８】そして、図３に示すように、電子マネー入金機２３の筐体の上部には、タッチパネル式の表示部２３４ａが操作性を考慮して所定の傾斜角を成して設けられており、また、表示部２３４ａと同様に所定の傾斜角を成して形成されている前面中央部のパネルには、電話機２３６，紙幣入金部２３２ａ，ＩＣカード（電子マネーカード）のカード挿入口２３３ａ及びジャーナル出力口２３５ａが設けられている。本例での電子マネー入金機２３は、主な機能として、ＩＣカード５への現金支払いによる入金機能、給与天引き支払いによる入金機能、現金による入金データ及び給与引きデータをサーバ（売上回収データ受付サーバ２５）へ送信する送信機能、及び残高照会機能を備えている。本例では、ＩＣカード５に入金できる限度額を支払い形態（現金支払い，給与天引き支払い）毎に設定しており、限度額以上の金額は入金できないようにしている。この限度額の情報は、カード発行時にＩＣカード５内に予め書込まれている。利用者のＩＣカード５に入金された入金データＭＤは、例えばタイマー起動による締め処理で、１日１回又は所定時間毎に分割して売上回収データ受付サーバ２５に送信されるようになっている。なお、電子マネー入金機２３側では記憶せずに、入金操作が終了した時点で管理会社２側に送信して売上回収データ受付サーバ２５に記憶するようにしても良い。或いは、売上回収データ受付サーバ２５側からの指令で入金データＭＤを収集するようにしても良い。

【００１９】図４は電子マネーＰＯＳ端末２４の構成の一例を示しており、図５はその外観図を示している。図４において、電子マネーＰＯＳ端末２４は、ＩＣカードのデータの読込み及び電子マネーデータ等の書換え等を行うためのＩＣカードリーダライタ２４２と、銀行カードやクレジットカード等のキャッシュレスカードのデータの読み書きを行うための磁気カードリーダライタ２４３と、ファンクションキー，テンキー等から成るキーボード２４４と、カード所持者が暗証番号の入力を行うためのコードレスタイプ（光通信式）の暗証入力用キーパッド（光通信テンキー）２４５と、取引内容や操作手順のガイダンス等を表示するための表示装置２４６と、支払い明細や売上げ明細をジャーナル印字するためのプリンタ２４７と、売上データ（暗号化した支払いデータ，及び回収データ）を記録するためのディスク装置２４８と、管理会社２側の売上回収データ受付サーバ２５とオンライン接続するための通信装置２４９と、各機器を制御するパソコンから成る制御部２４１とを備えている。

【００２０】そして、図５に示すように、電子マネーＰＯＳ端末２４の筐体の上部の前面パネルは所定の傾斜角を成して形成されており、表示部２４６ａ，操作部２４４ａ，銀行カード等のキャッシュレスカードの読取部２４３ａ及び記録媒体の装填部２４８ａが設けられており、筐体の下部の前面パネルには、ＩＣカード（電子マネーカード）のカード挿入口２４２ａが設けられている。そして、筐体の上部後方にはジャーナル出力口２４７ａが設けられ、更にその後方には暗証入力用キーパッ

ド２４５が装着されている。

【００２１】本例での電子マネーＰＯＳ端末２４は、商店街事務局や地域情報ＶＡＮ等とのオンラインネットワーク構築により、高度の顧客情報処理サービスの利用をも可能とするオンライン端末であり、主な機能として、ＩＣカードによる支払いデータを暗号化して回収データとともに蓄積する蓄積機能、ＩＣカードの記録エリアに利用履歴（入出金の取引ログ）を書込むログ機能、店舗専用のＩＣカードの暗号化プログラムによって回収データを暗号化し、支払いデータとともに売上データ（請求データ）として管理会社２側のコンピュータ（本例では売上回収データ受付サーバ２５）に送信する送信機能を備えている。この他に、提携店舗のサービス情報（割引率等の特典）や運用情報（請求締め日等）を設定する設定機能、売上げ等のジャーナル印刷機能を備えており、更に、プリペイドカード，銀行カード（銀行ＰＯＳ），クレジットカード及びポイントサービスが行えるサービスカードのカード処理機能を搭載している。

【００２２】電子マネーＰＯＳ端末２４のジャーナルには、利用者に渡される支払い明細の他に、日替集計、プリペイドカード種別の利用件数・金額，販売枚数，売上集計、銀行カード売上集計等が印字される。上記の売上データの送信機能は、店舗専用ＩＣカード６を用いた場合のみ使用できるようになっている。また、蓄積ファイル（売上データ）の記録媒体としては、本例では出し入れ持ち運び可能なリムーバブルディスク（フレキシブルディスク／書換可能光磁気ディスク等）が使用され、何らかの障害で売上データを管理会社２側に送信できない場合は、記録媒体の持ち運びにより店舗側に送ることができるようにしている。売上データの送信は、店舗用ＩＣカード６の所持者（店長等）の指示により、電子マネーＰＯＳ端末２４から１日１回又は所定の期間毎に行われる。

【００２３】上述のような構成において、先ず、電子マネー入金機２３の動作例を図６及び図７のフローチャートに沿って説明する。電子マネー入金機２３は、待機状態における初期画面として、例えば電子マネーが利用できる店舗の案内画面を表示部２３４ａに表示しており（ステップＳ１）、店舗の詳細案内のメニューが選択された場合は、ジャンル別の店舗の一覧を表示し、更に個別店舗が選択されたときには（ステップＳ２）、個別店舗の案内画面（広告等）を表示をする。そして、個別店舗の案内と共に表示されている電話記号部にタッチされた場合は、当該店舗の電話に自動ダイヤルする。この自動ダイヤル機能は、利用者に対するサービスの一環として設けられたもので、利用者が店に行く場合など、利用者は電話機２３６により当該店舗の店員と無料で会話することができる（ステップＳ３）。

【００２４】一方、入金のメニューが選択された場合には（ステップＳ４）、利用者に対してＩＣカードの挿入を促すガイダンスを表示し、ＩＣカードの挿入待ちとする（ステップＳ５）。そして、ＩＣカードが挿入されると、ＩＣカードリーダライタ２３３によりデータを読出し、本システムで発行された利用者カードか否かをＩＤデータにより確認した後、暗証番号の入力を促すガイダンスを表示部２３４ａに表示する（ステップＳ６）。暗証番号が入力されると、制御部２３１では、ＩＣカードのデータに含まれる暗証番号と入力された暗証番号とを照合して個人の認証を行い（ステップＳ７）、認証が取れたのであれば、図１０に示すように、現在の電子マネー残高、入金可能な限度額、入金方法の選択メニュー等を表示する（ステップＳ８）。

【００２５】本例では、入金方法として、現金による入金と給与天引きによる入金があり、利用者はいずれかを選択できるようになっている。先ず前者が選択された場合の処理を説明する。上記ステップＳ８において入金方法として現金による入金が選択され（ステップＳ９）、貨幣（本例では紙幣）が投入されたのであれば、投入金額を計数して表示し、ＩＣカードに入金する金額を入力する旨の表示をする（ステップＳ１０）。入金する金額が入力されたのであれば、限度額以内か否かを確認した後（ステップＳ１１）、金額の確認メッセージ（入金額，入金後の電子マネー残高，入金後の入金限度額）を表示して利用者に確認する（ステップＳ１２）。ステップＳ１２において取消しの指示がされたのであれば、カードを返却して動作を終了し（ステップＳ１３）、確認ＯＫの指示がされたのであれば、電子マネーＩＤを採番する。ここで、電子マネーＩＤは、電子マネーデータを書替える毎に付与される発行の番号であり、例えば、現金／給与天引きの区分，発行機を特定する番号，発行日を示す情報（例えば基準年月日を１日目とした連番）、発行機毎の連続番号等の情報から構成される。本例では、電子マネー入金機２３が電子マネー発行機に相当し、電子マネー入金機２３によって上記の各情報を更新して入金毎に電子マネーＩＤを採番する（ステップＳ１４）。

【００２６】そして、ＩＣカードの入金エリア内に、何回目の入金かを示す回数，電子マネーＩＤ，入金金額及び電子マネー残高を取引履歴として記録すると共に、ＩＣカードの限度金残高エリア内の残高（１月の給与からの引落し限度額，１月の現金利用限度額）及び限度額エリア内の入金可能限度額（給与限度額，現金限度額）を更新をする。ここで、利用履歴のエリアは、入金エリア及び出金エリアから成り、それぞれ複数回の取引を記録できるようになっており、サイクリックに使用される（ステップＳ１５）。そして、電子マネーの入金ログデータ（例えば、入金時の日付，利用者ＩＤ，電子マネーＩＤ及び入金金額）ＭＤを作成し、前述の送信機能により売上回収データ受付サーバ２５に送信する。ここでは、入金処理時に送信する場合を例としている。この入

金ログデータＭＤは売上回収データ受付サーバ２５の記憶手段にに記憶され、後述する集計決済端末における不正チェック処理（取引の正当性確認処理）において使用される。入金ログデータの送信が完了した後（ステップＳ１６）、投入金額と入金金額とを比較して釣り銭の有無をチェックし、釣り銭がある場合は釣り銭を投出して返却した後、入金された現金を金庫へ収納する（ステップＳ１７）。そして、入金明細のジャーナルを出力すると共に（ステップＳ１８）、カードを投出して返却し（ステップＳ１９）、入金処理を終了する。

【００２７】続いて、給与天引きによる入金処理について説明する。なお、現金により入金処理と同一の処理については簡略化して説明する。上記ステップＳ９において入金方法として給与天引きによる入金が選択されたのであれば、カード所持者により指定された入金金額を入力して限度額以内か否かを確認した後（ステップＳ２０）、金額の確認メッセージをを表示し、取消しの指示がされたのであれば、カードを返却して動作を終了し、確認ＯＫの指示がされたのであれば（ステップＳ２１）、電子マネーＩＤを採番し（ステップＳ２２）、ＩＣカードを更新する（ステップＳ２３）。そして、電子マネーの入金ログデータＭＤを作成して売上回収データ受付サーバ２５に送信し（ステップＳ２４）、ステップＳ１８へ移行して入金明細のジャーナルを出力すると共に、カードを返却し（ステップＳ１９）、入金処理を終了する。

【００２８】次に、電子マネーＰＯＳ端末２４の動作例を図８のフローチャートに沿って説明する。電子マネーＰＯＳ端末２４は、待機状態における初期画面として、各機能の選択画面が表示されている。ここでは、店舗情報等の設定機能と各種ジャーナルの印刷機能、及びクレジットカード等の一般的なキャッシュレスカードによる支払い処理については説明を省略し、ＩＣカード５による支払い処理と、売上データの送信処理（締め処理）について説明する。先ず、支払い処理について説明する。ステップ３０において、支払い処理が指示されたのであれば、利用者カードの挿入を促すガイダンスを表示してＩＣカードの挿入待ちとする（ステップＳ３１）。利用者のＩＣカードがカード挿入口２３３ａに挿入されると、電子マネーＰＯＳ端末２４の制御部２４１では、ＩＣカードリーダライタ２４２によりデータを読出し（ステップＳ３２）、本システムで発行された利用者カードか否かをＩＤデータにより確認した後、暗証番号の入力を促すガイダンスを表示部２４６ａに表示する。レジ担当者は暗証入力用キーパッド２４５をカード所持者に渡して暗証番号を入力してもらう。

【００２９】カード所持者により暗証番号が入力されると、制御部２４１では、ＩＣカード５のデータに含まれる暗証番号と入力された暗証番号とを照合して個人の認証を行い（ステップＳ３３）、個人認証が取れたのであれば、支払い金額の入力を促すガイダンスを表示する。レジ担当者により支払い金額（商品の購入金額）が入力されると（ステップＳ３４）、割引率が設定されている場合には割引額を計算し、割引後の支払い金額を算出する。この割引サービスは店舗毎に予め設定されている（ステップＳ３５）。そして、支払い金額とカード残高とを比較して残高不足でないかどうかを確信し（ステップＳ３６）、残高不足でなければ支払い金額を減額してＩＣカードを更新する。その際、入金エリア内の電子マネー残高を更新すると共に、ＩＣカードの出金エリア内に利用履歴（何回目の出金かを示す回数，電子マネーＩＤ，利用日時及び利用場所（店舗番号等））を記録する。

【００３０】そして、蓄積ファイルに回収データ（利用履歴の各情報、利用者ＩＤ等）を登録すると共に（ステップＳ３７）、ＩＣカードに支払いデータを送り、データの暗号化を指示する。ここで、上記の回収データと支払いデータは同一内容であり、上記の利用履歴の各情報及び利用者ＩＤ等から構成されている。ＩＣカードに記録されている暗号化プログラムでは、暗証番号により支払いデータをＤＥＳ型アルゴリズムを用いて暗号化する（ステップＳ３８）。制御部２４１では、暗号化された支払いデータを読出し（ステップＳ３９）、図１１に示すように、暗号化された支払いデータＳＤ２’を回収データＳＤ１とともに売上データとして蓄積ファイルに記憶すると共に（ステップＳ４０）、支払い明細を作成してプリンタ２４７によりジャーナル出力し（ステップＳ４１）、支払い処理を終了する。

【００３１】続いて、売上データの送信処理について説明する。上記ステップＳ３０において、締め請求指示がされた場合は、店舗用ＩＣカード６の挿入を促すガイダンスを表示部２４６ａに表示する（ステップＳ５１）。店舗用ＩＣカード６が挿入されると、制御部２４１では、本システムで発行された当該店舗のカードか否かをＩＤデータにより確認した後、暗証番号の入力を促すガイダンスをする（ステップＳ５２）。そして、入力された暗証番号とＩＣカード６のデータに含まれる暗証番号とを比較して取扱担当者（店舗担当者）の認証を行い（ステップＳ５３）、認証が取れたのであれば、蓄積された回収データを一件単位若しくはブロック単位でＩＣカード６に送り、暗号化を指示する（ステップＳ５４）。ＩＣカードの暗号化プログラムでは、暗証番号により回収データをＤＥＳ型アルゴリズムを用いて暗号化する。制御部２４１では、暗号化された回収データを読出して（ステップＳ５５）蓄積ファイルの回収データを書替える（ステップＳ５６）。そして、通信装置２４９を介して売上回収データ受付サーバ２５とオンライン接続し（ステップＳ５７）、図１２に示すように、暗号化された回収データＳＤ１’及び支払いデータＳＤ２’を売上データＳＤとして送信し、売上回収データ受付サー

バ２５のD／Bに記憶させる（ステップＳ５８）。そして、売上データＳＤの処理フラグを請求済みとし（ステップＳ５９）、売上データの送信処理を終了する。

【００３２】次に、集計決済端末２６の動作例を図１３及び図１４を参照して、図９のフローチャートに沿って説明する。なお、図１４（Ａ）及び（Ｂ）は、それぞれ売上回収データ受付サーバ２５に記憶される売上データＳＤと入金データＭＤのファイル構成の一例を示している。

【００３３】集計決済端末２６では、所定の期間例えば１月毎に店舗への振込みを行うための処理をする。先ず、売上回収データ受付サーバ２５から売上回収データＳＤ１’，ＳＤ２’を読出す（ステップＳ６０）。この時点では両データは暗号化されている。そして、電子マネー発行サーバ２２より店舗番号毎の復号キー（解除キー）ＫＷ１を取出し（ステップＳ６１）、この復合キーＫＷ１により回収データＳＤ１を復号する（ステップＳ６２）。そして、回収データＳＤ１にある該当利用者ＩＤを基に電子マネー発行サーバ２２より暗証番号ＫＷ２を読出し（ステップＳ６３）、この暗証番号ＫＷ２をキーに支払いデータを復号する（ステップＳ６４）。そして、それぞれのキーにより復号した回収データＳＤ１と支払いデータＳＤ２とを照合して一致するか否かを確認し（ステップＳ６５）、一致していない場合は、電子マネーカード若しくは店舗側の操作でデータの改ざんなどによる不正が行われたか、或いは他の何らかの原因によりデータの異常が発生したものと判断して異常有りの出力する。この場合は、不一致箇所などを示す詳細出力を基に、問題を調査する（ステップＳ６６）。

【００３４】上記ステップＳ６５において、回収データＳＤ１と支払いデータＳＤ２とが一致している場合は、利用者ＩＤと電子マネーＩＤを基に、売上回収データ受付サーバ２５に記憶されている入金データＭＤを読出し（ステップＳ６７）、同一電子マネーＩＤにおいて入金金額と出金金額とを比較して取引の正当性を確認する（ステップＳ６８）。そして、同一電子マネーＩＤにおいて入金＜出金の場合は異常と判断し、ステップＳ６６に移行して異常有りの出力する。一方、上記ステップＳ６８において入金≧出金の場合は正常と判断し（ステップＳ６９）、銀行振込みデータＢＤを作成し（ステップＳ７０）、店舗への確認用帳票を打ち出して処理を終了する（ステップＳ７１）。なお、銀行への振込みデータＢＤの送信は確認用帳票による店舗側の確認後行う。また、当該加盟団体へ給与天引きデータを送信する運用としている場合は、給与天引きのデータＰＤを加盟団体ＰＣ４へ送信する。

【００３５】なお、上述した実施の形態においては、カード発行機２１と電子マネー入金機２２を、別の機器として説明したが、同一装置としても良い。また、提携店１と管理会社２との間の通信回線は公衆電話回線に限るものではなく、専用線としても良い。

【００３６】

【発明の効果】以上に説明したように、本発明によれば、電子マネーＰＯＳ端末により利用者がプリペイドＩＣカードを使用する時に利用金額を利用者用のＩＣカードの暗号化プログラムによって暗号化し、さらに店カードを用いて売上げのデータを暗号化し、両者によって暗号化された１対のデータを綴めて管理会社に送り、管理会社側では、それぞれのデータを最初に登録された解除キーを用いて復号して両データの一致を取るとともに入金と出金の大小関係をチェックするようにしているので、カードの偽造／変造，店舗内における売上データの改ざん，伝送時のデータの改ざん等の不正行為に対して安全なプリペイドシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明の電子マネーシステムの全体構成の一例を示すブロック図である。

【図２】電子マネー入金機の構成の一例を示すブロック図である。

【図３】電子マネー入金機の外観構成の一例を示す斜視図である。

【図４】電子マネーＰＯＳ端末の構成の一例を示すブロック図である。

【図５】電子マネーＰＯＳ端末の外観構成の一例を示す斜視図である。

【図６】電子マネー入金機の動作例を説明するためのフローチャートである。

【図７】図６の分図である。

【図８】電子マネーＰＯＳ端末の動作例を説明するためのフローチャートである。

【図９】集計決済端末の動作例を説明するためのフローチャートである。

【図１０】電子マネー入金機の表示画面の一例である。

【図１１】本発明における不正のチェック方法を説明するための第１の図である。

【図１２】本発明における不正のチェック方法を説明するための第２の図である。

【図１３】本発明における不正のチェック方法を説明するための第３の図である。

【図１４】売上回収データ受付サーバに記憶される売上データ及び入金データのファイル構成の一例を示す図である。

【符号の説明】

１　提携店
２　管理会社
３　銀行ホストコンピュータ
４　加盟団体ＰＣ
５　プリペイドカード（ＩＣマネーカード）
６　店舗用ＩＣカード
７ａ，７ｂ，７ｃ　通信回線

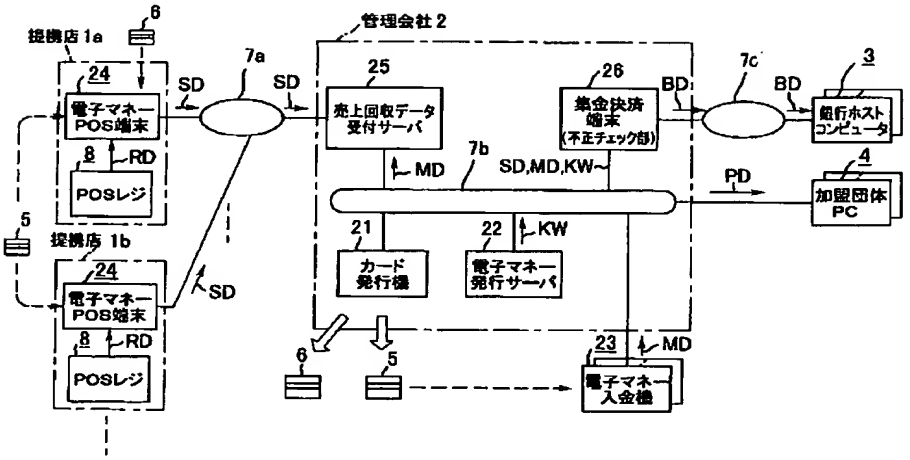
15

２１　カード発行機２１
２２　電子マネー発行サーバ
２３　電子マネー入金機

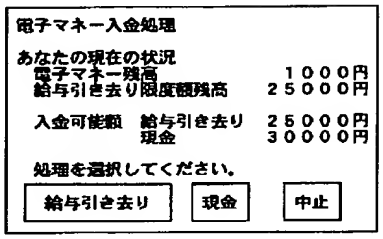
16

＊２４　電子マネーＰＯＳ端末
２５　売上回収データ受付サーバ
＊　２６　集計決済端末２６

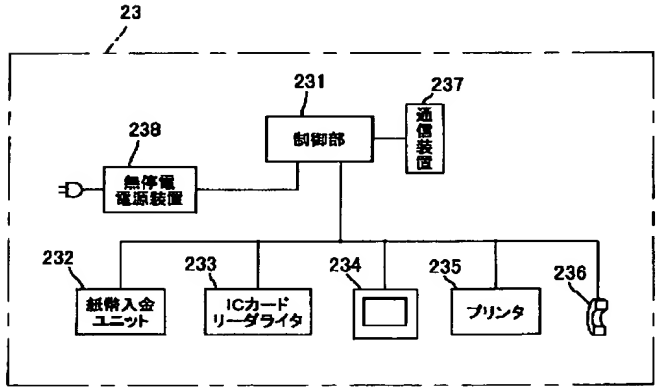
【図１】



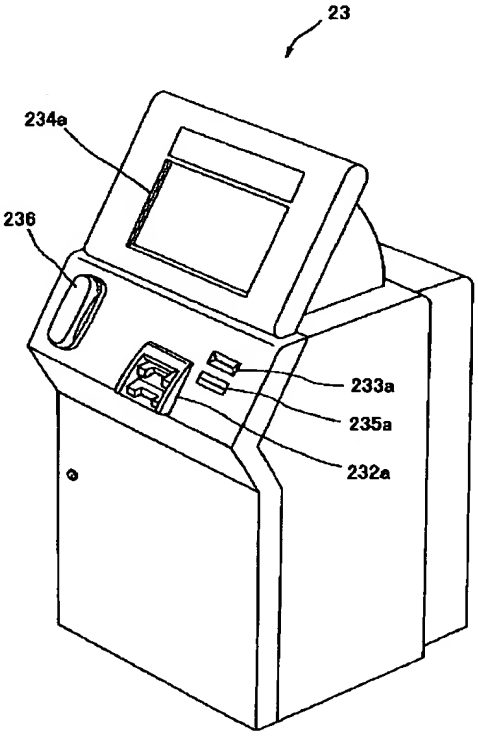
【図１０】



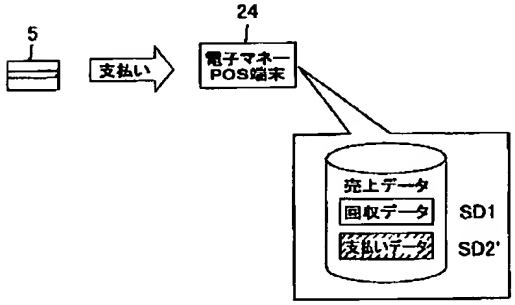
【図２】



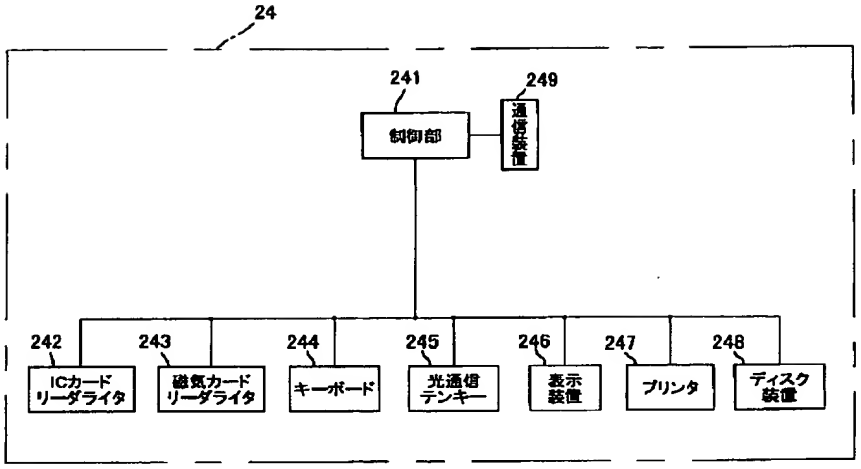
【図３】



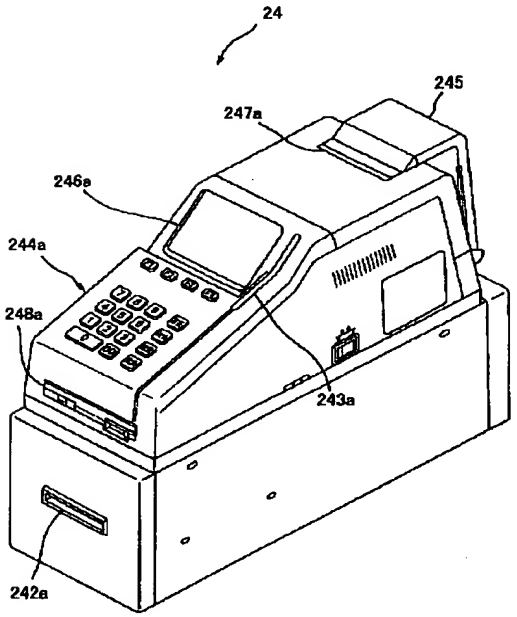
【図１１】



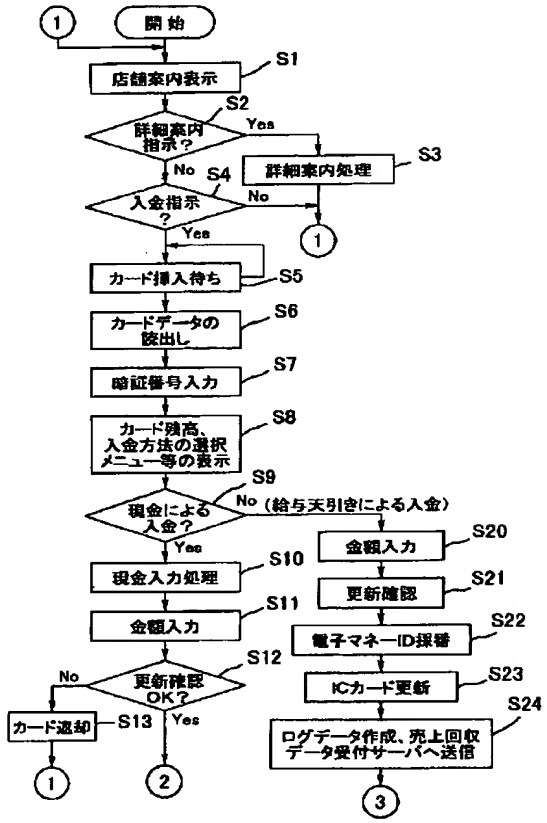
【図４】


24
241
249
制御部
通信装置
242
243
244
245
246
247
248
ICカード リーダライタ
磁気カード リーダライタ
キーボード
光通信 テンキー
表示 装置
プリンタ
ディスク 装置

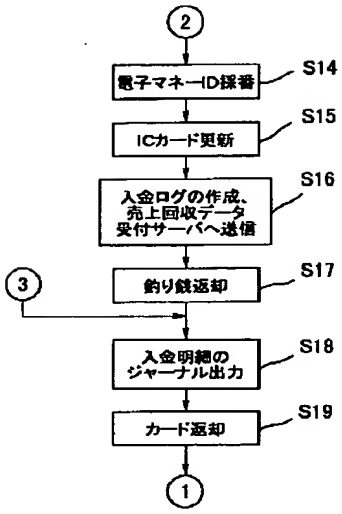
【図５】


24
245
247a
246a
244a
248a
243a
242a

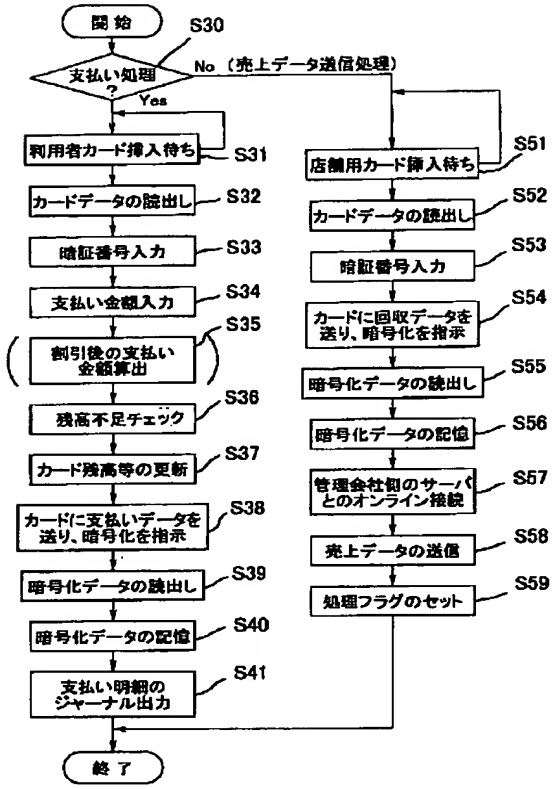
【図６】


開始
店舗案内表示
S1
詳細案内 指示？
S2
Yes
詳細案内処理
S3
No
入金指示 ？
S4
No
Yes
カード挿入待ち
S5
カードデータの 読出し
S6
暗証番号入力
S7
カード残高、 入金方法の選択 メニュー等の表示
S8
現金による 入金？
S9
No（給与天引きによる入金）
Yes
現金入力処理
S10
金額入力
S11
更新確認 OK？
S12
No
カード返却
S13
Yes
金額入力
S20
更新確認
S21
電子マネーID採番
S22
ICカード更新
S23
ログデータ作成、売上回収 データ受付サーバへ送信
S24
1
2
3

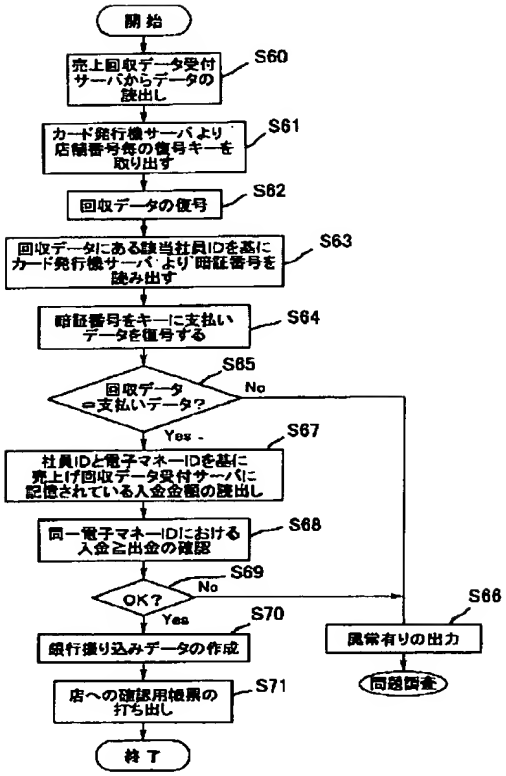
【図７】


2
電子マネーID採番
S14
ICカード更新
S15
入金ログの作成、売上回収データ受付サーバへ送信
S16
3
釣り銭返却
S17
入金明細のジャーナル出力
S18
カード返却
S19
1

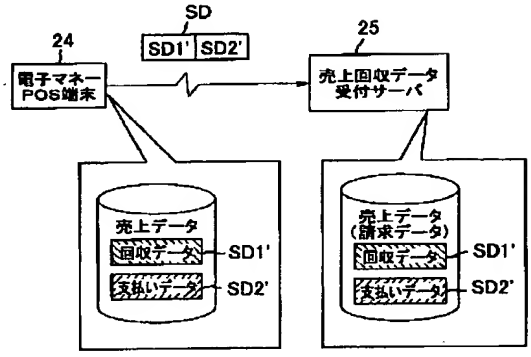
【図８】


開始
S30
支払い処理？
No（売上データ送信処理）
Yes
利用者カード挿入待ち
S31
カードデータの読出し
S32
暗証番号入力
S33
支払い金額入力
S34
割引後の支払い金額算出
S35
残高不足チェック
S36
カード残高等の更新
S37
カードに支払いデータを送り、暗号化を指示
S38
暗号化データの読出し
S39
暗号化データの記憶
S40
支払い明細のジャーナル出力
S41
店舗用カード挿入待ち
S51
カードデータの読出し
S52
暗証番号入力
S53
カードに回収データを送り、暗号化を指示
S54
暗号化データの読出し
S55
暗号化データの記憶
S56
管理会社側のサーバとのオンライン接続
S57
売上データの送信
S58
処理フラグのセット
S59
終了

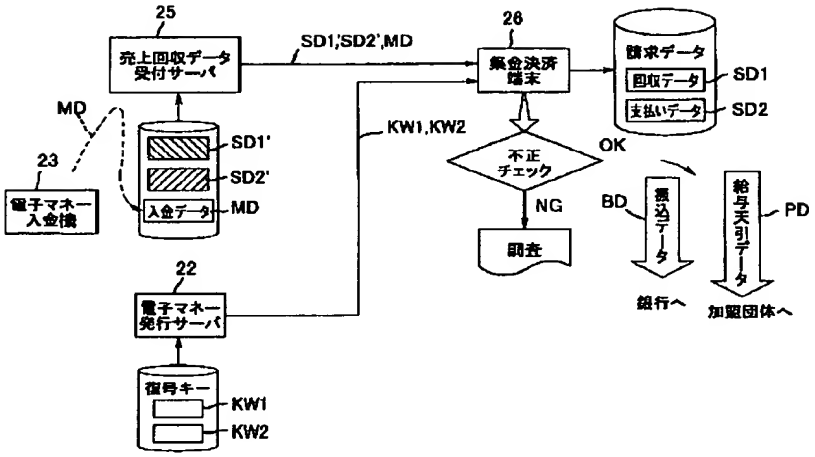
【図９】


開始
売上回収データ受付サーバからデータの読出し
S60
カード発行機サーバより店舗番号毎の復号キーを取り出す
S61
回収データの復号
S62
回収データにある該当社員IDを基にカード発行機サーバより暗証番号を読み出す
S63
暗証番号をキーに支払いデータを復号する
S64
回収データ＝支払いデータ？
S65
No
Yes
社員IDと電子マネーIDを基に売上げ回収データ受付サーバに記憶されている入金金額の読出し
S67
同一電子マネーIDにおける入金と出金の確認
S68
OK？
S69
No
Yes
銀行振り込みデータの作成
S70
店への確認用領収書の打ち出し
S71
終了
異常有りの出力
S66
問題調査

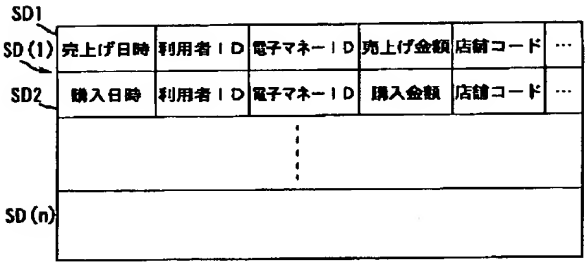
【図１２】


SD
SD1'
SD2'
24
電子マネーPOS端末
25
売上回収データ受付サーバ
売上データ
回収データ
SD1'
支払いデータ
SD2'
売上データ（請求データ）
回収データ
SD1'
支払いデータ
SD2'

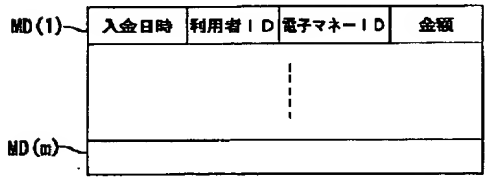
【図１３】


25
売上回収データ受付サーバ
SD1,SD2',MD
26
集金決済端末
請求データ
回収データ
SD1
支払いデータ
SD2
MD
23
電子マネー入金機
SD1'
SD2'
入金データ
MD
KW1,KW2
不正チェック
OK
NG
調査
BD
振込データ
銀行へ
給与天引データ
PD
加盟団体へ
22
電子マネー発行サーバ
復号キー
KW1
KW2

【図１４】


SD1
SD(1)
売上げ日時
利用者ＩＤ
電子マネーＩＤ
売上げ金額
店舗コード
…
SD2
購入日時
利用者ＩＤ
電子マネーＩＤ
購入金額
店舗コード
…
SD(n)

(A)


MD(1)
入金日時
利用者ＩＤ
電子マネーＩＤ
金額
MD(m)

(B)